

Title (en)
Improved variants of the Fiat-Shamir identification and signature scheme.

Title (de)
Varianten des Fiat-Shamir-Verfahrens zum Identifizieren und Unterschreiben.

Title (fr)
Variantes du procédé Fiat-Shamir pour identifier et pour signer.

Publication
EP 0325238 B1 19940105 (EN)

Application
EP 89100825 A 19890118

Priority
US 14540288 A 19880119

Abstract (en)
[origin: EP0325238A2] A method of proving the identify of an entity comprising the steps of establishing a public key for the entity consisting of a modulus n which is the product of at least two prime numbers, and a sequence of k numbers v_1, \dots, v_k (10); computing a private key (12) for the entity consisting of k numbers s_1, \dots, s_k satisfying $s_j \cdot d^{v_j} \equiv 1 \pmod{n}$ for all $1 \leq j \leq k$, where d is a universally known constant larger than 1; transmitting from the entity to a verifier (20) $x = r \cdot d^x \pmod{n}$ (16,18) where r is a random number in the range $0 < r < n$; transmitting from the verifier (20) to the entity a sequence of k random numbers e_1, \dots, e_k in the range $0 < e_j < d$ (22,24); transmitting from the entity to the verifier (20) the value $\langle \text{MATH} \rangle \pmod{n}$ (32); and verifying the identity of the entity by checking that $\langle \text{MATH} \rangle \pmod{n}$ (54). i

IPC 1-7
G07F 7/10

IPC 8 full level
G09C 1/00 (2006.01); **G07F 7/10** (2006.01); **H04L 9/00** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)
G07F 7/1016 (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); **H04L 9/3218** (2013.01 - EP US); **H04L 9/3247** (2013.01 - EP US)

Cited by
USRE42517E; US7184547B1; US5987138A; EP0505302A1; EP0518365A3; FR2773406A1; EP1056241A3; EP0461983A1; FR2663141A1; EP0502559A3; AU648643B2; EP0496459A1; AU650321B2; US5452357A; US7590846B2; AU677269B2; KR101142656B1; EP0801480A1; FR2747257A1; US5799088A; EP0427601A1; FR2654288A1; US5563948A; WO9213321A1; WO9515633A1; WO9415423A1; WO9214318A1; US8239957B2; US8856942B2

Designated contracting state (EPC)
AT BE CH DE ES FR GB GR IT LI LU NL SE

DOCDB simple family (publication)
EP 0325238 A2 19890726; EP 0325238 A3 19900829; EP 0325238 B1 19940105; AT E99818 T1 19940115; AU 2859789 A 19890720; AU 631111 B2 19921119; CA 1331642 C 19940823; DE 68911935 D1 19940217; DE 68911935 T2 19940428; ES 2049764 T3 19940501; JP H01309088 A 19891213; JP H0750375 B2 19950531; US 4933970 A 19900612

DOCDB simple family (application)
EP 89100825 A 19890118; AT 89100825 T 19890118; AU 2859789 A 19890118; CA 588548 A 19890118; DE 68911935 T 19890118; ES 89100825 T 19890118; JP 961889 A 19890118; US 14540288 A 19880119